PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2003-248578**
(43)Date of publication of application : **05.09.2003**

(51)Int.Cl. **G06F 7/58**
G06K 19/10
G09C 1/00

(21)Application number : **2002-347277**
(22)Date of filing : **29.11.2002**

(71)Applicant : **STMICROELECTRONICS SA**
(72)Inventor : **WUIDART LUC**
BARDOUILLET MICHEL
PLAZA LAURENT

(30)Priority
Priority number : **2001 200115529** Priority date : **30.11.2001** Priority country : **FR**

(54) GENERATION OF SECRET QUANTITIES OF INTEGRATED CIRCUIT IDENTIFICATION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method and a circuit for generating a secret quantity based on an identifier of an integrated circuit.
SOLUTION: A first digital word is generated from a physical parameter networkand the first word is submitted to at least one shift registerthe output of the shift register generating the secret quantity.

CLAIMS

[Claim(s)]
[Claim 1]In a method of generating secret quantity (KEY) based on an identifier of an integrated circuit (2)A methodwherein an output of said shift register forms said secret quantity including a step which generates the first digital wordand a step which shows at least one retroactivity shift register (6) said first word from a physical parameter network (3).
[Claim 2]A method of showing two or more retroactivity shift registers (6) said first

wordchoosing one of these shift registersand forming said secret quantity (KEY) according to claim 1.
[Claim 3]A method according to claim 2wherein said selection is changed after cancellation of secret quantity of precedence.
[Claim 4]A method according to claim 1wherein said shift register (6) is a linearity retroactivity shift register.
[Claim 5]A method of choosing one of two or more shift registers by a selector (7) according to claim 1.
[Claim 6]A circuit which generates secret quantity (KEY) inside an integrated circuit (2)comprising:
A generator (4) of the first digital word specific to an integrated circuit chip based on a physical parameter network (3).
At least one retroactivity shift register (6) which receives said first word as an input and provides said quantity.
It is programmable by a counter (9) and is a selector of a drift sequence of said shift register.

[Claim 7]A circuit which generates secret quantity (KEY) inside an integrated circuit (2)comprising:
A generator of the first digital word specific to an integrated circuit chip based on a physical parameter network (3).
A retroactivity shift register (6) which accepts said first binary word as an input.
A selector (7) which chooses one of said shift registers which provide said secret quantity.

[Claim 8]The circuit according to claim 6 when restricted data is canceled selection performed by said selectorwherein it is changed.
[Claim 9]The circuit according to claim 7wherein a selector (7) is formed of a multiplexer which chooses an input/output to an input or an output of said shift register (6).
[Claim 10]A circuit which a register (58) which memorizes a word and said secret quantity of said beginning in the circuit according to claim 6 is a temporary registerand is characterized by said circuit containing a means (12) to reset these temporary storage elementsafter beforehand fixed time.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to use of the secret quantity to which it

comes from the electronic subassembly element which comes from an integrated circuit or includes such a circuit. For examplethis invention relates to the use of such secret quantity by a program like an encryption key as secret quantity of the process of discernment of an integrated circuitor attestation. More specificallythis invention relates to the use of the digital identifier of an integrated circuit which comes from a physical parameter network relevant to manufacture of an integrated circuit chip.
[0002]
[Description of the Prior Art]For exampleuse of the identifier which comes from the physical parameter network for coding the data provided with an integrated circuit chip by attestation or itIn order to make it possible to use the binary word hidden or embedded into the integrated circuit for the storage cell to which it may be copied illegallywithout making it memorize temporarilyit has been taken further seriously. Thereforethe reliability of the system which may happen and which is received unjustly improves. Use of a physical parameter network makes it possible to obtain a digital identifier different mutually for a different integrated circuit chip which comes from given manufacture.
[0003]Generallyin order to transmit to a remote systemthe digital identifier of an integrated circuit is provided out of a circuitcoding or after scramble was carried outand after [possible]. The latter (scramble) uses the received word and does not need to get to know an identifier.
[0004]The application of this invention is related with the smart card field used for the financial transaction from the account unit (countunit) which is not prepaid one or prepaidand there are some which shall not contact a smart card reader in the communication.
[0005]Another application is a data transmission system which uses the decoder specified as the user side by the individual. In such a casea decoder may also include the authentication circuit using the identifier which comes from the physical parameter network of the integrated circuit contained there. When a metaphor of the smart card in a payment system explainsthe point that attestation is performed by different system from a reader is the same as connecting the smart card with user levels to a readerwithout changing.
[0006]The disadvantage of using the identifier which comes from a physical parameter network is connected with the individual and fixed character.
[0007]Thereforewhen a trespasser succeeds in the piracy to the digital word (the amount of attestationor a coding key) containing an identifier or this identifierthere is no solution besides changing an integrated circuit. When it is actually suspected that piracy was made by the identifierin safe applicationit is desirable to stop use of the identifier of ****. This phenomenon is generally used as a coding keyattestationor a general twist target with cancellation of secret quantityand is known.
[0008]The lack of solution to the cancellation of a key or secret quantity based on use of the physical parameter network of an integrated circuit has restricted use of

these identifiers advantageous to many uses besides the present.
[0009]
[Problem(s) to be Solved by the Invention]The purpose of this invention is to conquer the known problem of the digital identifier which comes from the physical parameter network in an integrated circuit.
[0010]More specificallythe purpose of this invention is to make it possible to cancel without changing the integrated circuit which has relation in the secret quantity or the key based on the identifier which comes from a physical parameter network.
[0011]When cancelingthe number of usable digital identifiers may be increased by increasing the number of physical parameter networks. Howeversuch solution has the problem that an integrated circuit will become large. And there are still very few identifiers which can be used.
[0012]The size of larger secret quantity than the size of the word to which it comes from a physical parameter network has a possibility that it may be searched.
[0013]Another purpose of this invention is to provide the solution which does not eliminate each characteristic of an integrated circuit identifier with a physical parameter network.
[0014]An object of this invention is to provide the solution which is compatible with the miniaturization of an integrated circuit.
[0015]In order to make secret quantity still saferthis invention is transparent for the secret quantity utilization system sidethat isan object of this invention is to provide the solution which does not need to know a means by which the latter (side to be used) is used.
[0016]
[Means for Solving the Problem]A step which this invention makes generate the first digital word from a physical parameter network in order to attain the purpose of these and othersA method of generating secret quantity based on an identifier of an integrated circuitwherein an output of said shift register forms said secret quantity is provided including a step which shows at least one retroactivity shift register said first word.
[0017]According to the embodiment of this inventiontwo or more retroactivity shift registers are shown said first wordand it is chosen in order for one of these registers to form secret quantity.
[0018]According to the embodiment of this inventionlet said selection be the thing by which secret quantity of precedence was canceled and which is back-changed.
[0019]According to the embodiment of this inventionsaid one or more shift registers are linearity retroactivity shift registers.
[0020]According to the embodiment of this inventionwhile a shift register has more than one by a selectorit is chosen from from.
[0021]A generator of the first digital word in which this invention is specific to an integrated circuit chip based on a physical parameter network againAt least one

retroactivity shift register which receives said first word as an input and provides said quantityIt aims at providing a circuit which generates secret quantity inside [by which a selector of a derivation sequence (derivation sequence) of said programmable shift register being included with a counter] an integrated circuit.
[0022]A generator of the first digital word to an integrated circuit chip based on a physical parameter network in which this invention is still more specificSome retroactivity shift registers which shall accept said first binary word as an inputIt aims at providing a circuit which generates secret quantity inside [containing a selector which chooses one of said two or more retroactivity shift registers which provide said secret quantity] an integrated circuit.
[0023]According to the embodiment of this inventionselection performed by said selector shall be changed when canceling restricted data.
[0024]According to the embodiment of this inventiona selector is formed of a multiplexer which chooses an input or an output from the input/output of a shift register.
[0025]According to the embodiment of this inventiona register which memorizes a word and said secret quantity of said beginning is a temporary registerand said circuit contains a means to reset those temporary storage elements after beforehand fixed time.
[0026]In explanation of a specific embodiment which is not limited to below in relation to an accompanying drawingthe purposethe featureand an effect which this invention mentioned above are explained in full detail.
[0027]
[Embodiment of the Invention]In order to clarifywith the element of an integrated circuitonly a thing required for an understanding of this invention is illustratedand it is explained henceforth. It is the component part of an integrated circuit or an electronic subassembly elementandspecificallythe portion without regards to generating secret quantity with the physical parameter network characteristic of this invention is not shown. Since it is applicable to all the conventional methodsabout use (for examplebased on the process of attestation or coding) of secret quantitythis invention was not concerned within and without the integrated circuitand is not explained in full detail.
[0028]It connects [the physical parameter network which provides the first digital word relevant to / in the feature of this invention / manufacture of the integrated circuit for at least one shift registerand] to linearity retroactivity preferablyIt is forming the secret quantity of an integrated circuit using the digital word provided with said shift register.
[0029]According to this inventiontwo or more linearity retroactivity shift registers are used functionally. The number of registers may be physically increased in generating of an integrated circuitor a single shift register may be providedand derivation of a bit which is different so that it may be stated henceforth may be provided.

[0030]Drawing 1 expresses briefly the embodiment of the cell 1 for generating the secret cuantity (KEY) of the integrated circuit 2 with the block.
[0031]The cell 1 contains the physical parameter network 3 (PPN) in connection with manufacture of an integrated circuit chip. The physical parameter network 3 provided many signalsand expressed said physical parameter networkwas temporarily memorized by the storage element 5 (REG1)and is connected with the circuit 4 which extracts binary word.
[0032]For exampleall the parameters containing an electrical measurement parameter can be used. Measurement of the threshold voltage of a transistormeasurement of resistance or measurement of stray capacitancemeasurement of the current generated by the current sourcemeasurement of a damping time constant (for exampleintegrated circuit)measurement of vibrational frequencyetc. may be sufficient as it. Since those characteristics of an integrated circuit are technical and it is easily influenced by dispersion in a manufacturing processit is thought that the electric parameter taken into consideration is specific to the manufactureand forms the signature of the integrated circuit.
[0033]In the example of electric parameter measurementa signal may be changed into a digital signal by an analog-digital converterand said converter may form the binary word which multiplexes including the extracting circuit 4 and is memorized by the register 5.
[0034]The circuit which uses a time test can also be used as a physical parameter network. For exampleread-out/writing time of an EEPROM type memory are measured. The example of this kind of physical parameter network is shown in US5818728Band was considered as reference of this invention.
[0035]The physical parameter network based on a flip-flop as shown in the France patent application No. 0104585 considered as reference of this invention can also be used further.
[0036]According to this inventionthe key KEY is obtained by showing a linearity shift register the binary word extracted from the physical parameter network.
[0037]According to the embodiment shown in drawing 1the n linearity shift registers 6 (LFSR1LFSRi...LFSRn) are shown. Each output of a different register is sentfor example to the selector 7 (SEL)and the output provides said secret quantity in the temporary storage element 8 (REG2). Or the selector 7 may be arranged in the not the lower stream but upper stream of the register 6.
[0038]Based on the binary parameter-ized word generated by the counter 9 (COUNT)selection of the linearity register usedi.e.control of the selector 7is performedandthereforesaid counter attaches a condition to the present secret quantityi.e.the quantity used until it is canceled. Other arbitrary conventional means may be [multiplexer] sufficient as a selector.
[0039]After cancellation of the data used last timewhenever restricted data is changedstepping of said counter is carried out. The counter 9 is the modulo numerical

value n of a shift register.
[0040]As for the cell 1it is desirable that it is in the safe portion of the integrated circuit 1. "A safe portion" is a portion protected from the attack by direct electrical measurement. For examplethe cell embedded to resin may be sufficient as it so that a cell may be canceled with a melting temperaturewhen a trespasser tries to detect the contents.
[0041]According to another embodiment which is not illustratedthe single linearity shift register in which the drawn bit is parameterized is used. This feature becomes further clear in connection with drawing 2 and drawing 3 henceforth.
[0042]The generating cell 1 contains the central unit 12 for controlling further a different element which forms it (CU). When required [the control signal of generating of secret quantity]in order that the central unit 12 may receive by a desirable temporary methodIn order to receive a control signal required for generating of the new secret quantity after cancellationi.e.the control signal which induces the increase in the counter 9 (or reduction)it communicates with the remaining portion of an integrated circuit with other portions.
[0043]The point that it is not necessary to learn how for the system which uses secret quantity to only process the secret quantity KEYand to generate it attracts attention. Thereforeto use of secret quantitythe generating cell by this invention is transparentand has all conventional directions and compatibility.
[0044]The counter 9 is replaced with the list of select codes of the multiplexing device which forms the selector 7 as other methods. These codes are memorized by nonvolatile memory in a parameterization stage in advance of use.
[0045]Realization is [that use of a linearity shift register enables cancellation of secret quantity] easyIt has the advantage that it is desirable more concretely at the point which enables change of the secret quantity of an integrated circuit when canceling the quantity of precedenceand the identifier which comes from a physical parameter network is used on the other handand it cannot infringe in particular on such an identifier by electrical measurement.
[0046]Drawing 2 is an overall lineblock diagram of a retroactivity shift register. Such a register comprises two portionsthe shift register 20 and the retroactivity function 21 (RETROACT)fundamentally. The shift register 20 forms continuation of the bit B1B-2B3...Bm--1and Bm like arbitrary shift registers. The function of the block 21 which forms a retroactivity function is calculating the input bit of a shift register (bit Bm) based on at least a part of combination of the bit contained in a register for every shift of continuation of a bit. Thereforethe retroactivity function 21 can be individually provided with each bit of the shift register 20. The output of the shift register 20 is formed of the least significant bit B1 of the binary word of this register with straight-line. According to the embodiment of a parallel outputthe value of all the bits of said shift register or a part of these bits are simultaneously sampled by the searched word.
[0047]The realization divides use of a shift register and it is preferred at an easy

point. The arbitrary conventional functions can be used as a retroactivity function. If it is possible to generate a word refreshable as an outputuse of a nonlinear retroactivity function may be taken into consideration. Howeveraccording to the embodiment of this inventionthe linearity retroactivity function which combined some bits of said shift register with the XOR type is used. The list of these bits is generally shown by the expression "a derivation sequence (deriving sequence)" or "Fibonacci composition (Fibonacci configuration)."

[0048]The repetitive period of the binary word contained in a shift register is based on the retroactivity function used not only in the number of bits of this register. In the linearity shift register of m bitthe binary sequence from which 2^m-1 differs can be used. That isthe secret quantity of the size of a before [2^m-1 bit] can be obtained by loadir g the continuous bit provided on the output OUT of the register of adaptation size. This is before repetition and forms the longest word. The fact which uses cor tinuation of the unloading of the code provided with the linearity shift register makes it possible to lengthen secret quantity about the word length provided by the physical parameter network.

[0049]In order to operate intelligiblydrawing 3 expresses briefly the 4-bit linearity shift register whose derivation sequences are B1 and B4. That isit is contained in register 20' and B1 and B4 over 4 bits which are each a least significant bit and a most significant bit are combined by XOR type gate 21' which forms a retroactivity function. The output of gate 21' forms a shift register inputandthereforeturns into B4 input. The output sequence OUT is provided by a least significant bit (B1).

[0050]If the state 1 is loaded to B4 after getting it blocked and resetting all other bits to 0if it assumes that a value is initialized as 1000The contents which register 20' followed are set to 1000; 1100; 1110; 1111; 0111; 1011; 0101; 1010; 1101; 0110; 0011; 1001; 0100; 0010; 0001 in front of ******.

[0051]According to this inventionselection of the derivation frequency before repetition by the number of possible combination can be performed if it is a person skilled in the art. realization of a linearity shift register -- hardware or software -- whichever it is a formit is completely as usual. for examplethe 395- published by the Bruce Schneier work considered as reference of this inventionand Wiley -- the 401st page and the 2nd edition of "application cryptography" can be referred to.

[0052]The word which comes from the network 3 and is used for setting out of the initial sequence of the register 6 is in-series or paralleland can be loaded. By setting up the initial value of the register 6it is controlled by the unit 12 and the number of the shift registers which are the conditions decided beforehand preferably provides the last word acquired by the refreshable method.

[0053]By changing a derivation sequence (it is the same as choosing the one more register 6 of continuation of n of drawing 1)said word acquired for the same input word (it has same larger number than m of shift cycles) is changed. As other methodsin order to change secret quantitythe number of shift cycles may be changed.

[0054]
[Effect of the Invention]The advantage of this invention is a point which can solve the problem about cancellation of the secret quantity obtained from the binary word which comes from a physical parameter network without providing a data utilization system with the element of a cancellation prevention method (anti-revocation procedure). Thereforethe solution provided by this invention is especially reliableand safe.
[0055]The advantage of this invention is a point that one physical parameter network can be usedrecognizing cancellation of some keys.
[0056]Another advantage of this invention is a point that the volatile characteristic (temporary) of secret quantity based on extraction of the word to which it comes from a physical parameter network can be held.
[0057]Of courseif this invention is a person skilled in the artvarious changeschangean improvementetc. will think of it easily. The length of the binary word used is based on applicationandspecificallyis based on the authentication process intrinsically used for an integrated circuit. In this pointit can be said that this invention has the existing utilizing method and compatibility of secret quantity with which the integrated circuit was provided.
[0058]Realization of the operation of a retroactivity shift register according to the functional guidance described above is not based on whether it is linearitybut if it is a person skilled in the artit can be performed. Selection of whether two or more shift registers are used or to use one register and the derivation sequence chosen by a switch can be performed by whether it is desirable to give priority to what between a storage cell and a shift register.
[0059]If the number of shift cycles is the same to a given keyit is not important. Even if setting out of other numbers of cycles is also possible in the case of change of the key accompanying cancellation and it continues the same derivation sequenceit is not necessary to carry out.
[0060]Finallyalthough this invention has so far explained relation with realization of hardware in more detailit is realizable also as a means of software.
[0061]It is going to carry out such changecorrectionand improvement in the portion of this indicationand they are performed in the thought of this inventionand the range. Thereforethe description mentioned above is only as an exampleand it is not going to limit it. Although Claims and its equivalent range prescribe this inventionit is limited to seeing.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is the schematic diagram which expressed the embodiment of the circuit

for generating the secret quantity by this invention with the block.
[Drawing 2]It is a block diagram of the linearity retroactivity shift register used in the circuit of drawing 1.
[Drawing 3]It is an easy example of the linearity retroactivity shift register in which the 1st and the 4th bit were drawn and which is 4 bits.
[Description of Notations]
1 Cell
2 Integrated circuit
3 Physical parameter network
4 A generatoran extracting circuit
5 A registera storage cell
6 A retroactivity shift registera linearity shift register
7 Selector
8 A registera temporary storage element
9 Counter
12 Central unit
20 Shift register
20'register
21 Retroactivity function
21'gate